Fallstudie „Der Staat als Big Brother“

Team Adleman: Sven-Philip Frick, Pascal Beyeler, Farhan Fayyaz, Pascal Murbach und Zeljko Jovanovic

Der Staat als Big Brother?

Freitag 06. Januar 2012, ab 20:30 im Kaufleuten Zürich

Moderator: Reto Lipp

Teilnehmer:

- Michael Leupold, Direktor des Bundesamts für Justiz
- Kurt Blöchlinger, ehemaliger Chef Bundeskriminalpolizei
- Seth Schoen, Mitglied des Vorstands der Electronic Frontier Foundation
- Pascal Lamia, Leiter Melde- und Analysestelle Informationssicherung Melani des Bundes
- Hanspeter Thür, Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
- Denis Simon, Präsident der Schweizer Piratenpartei.

Programm:

19:00 – 19:15 Eröffnungsrede
Reto Lipp

19:20 – 19:40 „Notwendige Massnahmen zur Sicherung einer funktionierenden Strafverfolgung“
Kurt Blöchlinger

19:45 – 20:05 „Warum die Privatsphäre auch im Zeitalter des Terrorismus ein unabdingbares Recht sein muss“
Seth Schoen

20:05 – 20:20 Pause

20:20 – 21:30 „Der Staat als Big Brother“
Moderierte Podiumsdiskussion mit allen Teilnehmern

Ab 21:30 Fragen aus dem Publikum

Zeitungsartikel

Werden sich die Visionen des britischen Schriftstellers ***George Orwell*** **bewahrheiten oder handelt es sich hierbei bloss um ein von Paranoia geprägtes Gedankenkonstrukt, das in keiner Weise adäquat begründet werden kann?**

Besteht also Anlass zur Besorgnis oder können wir uns entspannt zurücklehnen, weil vom Staat hinsichtlich Überwachung keine konkrete Gefahr ausgeht?

Diesen Fragen wird anlässlich einer öffentlichen Podiumsdiskussion am 6. Januar von 19:00 Uhr bis 21:30 Uhr im Kaufleuten nachgegangen.

An der Debatte werden Vertreter aus Politik, Wirtschaft und Forschung ihre Sicht der Dinge darlegen und versuchen zu ermitteln, was dafür spricht, dass uns ein Überwachungsstaat ins Haus steht oder ob und inwiefern diese Auffassung entkräftet werden kann.

Der SF-Wirtschaftsredaktor Reto Lipp wird eine kurze Einführungsrede halten und die geladenen Teilnehmer kurz vorstellen.

Es werden Referate vom ehemaligen Chef der Bundeskriminalpolizei und dem Mitglied **des Vorstands der Electronic Frontier Foundation, Seth Schoen, gehalten und anschliessend findet die eigentliche Podiumsdiskussion mit allen Teilnehmern statt, wobei das Publikum ebenfalls eingeladen ist, am Diskurs teilzunehmen, der sicherlich interessante Erkenntnisse hervorbringen wird.**

Wie sehen Sie das? Wenn Sie Sich fragen, was das alles soll, dann ist der Besuch dieser Podiumsveranstaltung empfehlenswert.

Glossar

Privatsphäre
Privatsphäre ist ein schon seit der Antike bekanntes Konzept, dass das Recht einer Person auf einen selbst bestimmbaren, nicht-öffentlichen Bereich definiert, in dem diese sich frei entfalten kann. In diesem (privaten) Bereich kann die Person frei handeln, ohne Angst vor Auswirkungen (z.B. Bewertung durch Dritte) haben zu müssen. Durch den technischen Fortschritt und die grosse Menge an verfügbaren Informationen, ist die Privatsphäre als solche in den Fokus der breiten Öffentlichkeit gekommen.

Big Brother
Der Begriff „Big Brother“ wird als Synonym für den Überwachungsstaat verwendet und stammt aus dem Roman „1984“ von George Orwell. Der Begriff ist stark emotional behaftet und richtet sich häufig gegen Institutionen welche legal oder illegal Eingriffe in die Privatsphäre vornehmen.

Datenschutz
Datenschutz bezeichnet technische und rechtliche Vorkehrungen zum Schutz von personbezogenen Daten. Rechtliche Grundlage hierfür ist das Recht auf den Schutz der Privatsphäre; die Umsetzung erfolgt in den meisten Ländern in entsprechenden Datenschutzgesetzen, welche mehr oder weniger ausgeprägt ausfallen. Der Datenschutz kann bei zuwiderlaufenden höheren Interessen (z.B. der Strafverfolgung) teilweise oder auch ganz aufgehoben werden.

Biometrische Daten
Körperliche Merkmale wie etwa ein Fingerabdruck oder die DNA, die für die eindeutige Identifikation einer Person genutzt werden können, werden als Biometrische Daten bezeichnet. Sie finden neuerdings grosse Verbreitung in Identitätsausweisen wie z.B. Reisepässen; ihre Erhebung und Verwendung wird kontrovers diskutiert.

Bundestrojaner
Als Bundestrojaner wird umgangssprachlich ein Trojaner bezeichnet, der von staatlichen Stellen im Zuge der Durchführung einer Quellen-TKÜ oder einer Onlinedurchsuchung verwendet wird. Der Trojaner wird dabei von Behörden wie etwa der Polizei auf den Computer eines Verdächtigen platziert und kann dann zum Aufzeichnen von Kommunikation und Sicherstellen von Daten verwendet werden.

Verschlüsselung
Als Verschlüsselung bezeichnet man ein Verfahren zum Umwandeln von Text (oder Daten allgemein) mithilfe eines Schlüssels in eine für Uneingeweihte nicht nutzbare Form. Verschlüsselungen werden zum Schutz von Kommunikation im Internet verwendet oder auch um Daten auf Datenträgern vor dem Zugriff Dritter zu schützen. Starke Verschlüsselungen stellen für staatliche Stellen ein Problem bei der Strafverfolgung dar, da diese keinen Zugriff auf den Inhalt der verschlüsselten Daten haben.

Computerkriminalität
Unter diesen Begriff fallen alle Straftaten, zu deren Durchführung ein Computer verwendet wurde. Die Zunahme der Computerkriminalität führte dazu, dass Strafverfolgungsbehörden die klassischen Ermittlungsmassnahmen auf den Bereich IT ausweiten mussten.

Quellen-TKÜ
Bei der Quellen-Telekommunikationsüberwachung wird mittels Software laufende Kommunikation über einen Computer mitgeschnitten. Die Quellen-TKÜ ist eine Reaktion des Gesetzesgebers auf die breite Verwendung von Computern zur Kommunikation und entspricht vom Typ her der Telefonüberwachung; je nach eingesetzter Software gehen die Möglichkeiten jedoch weit über diesen Zweck hinaus.

Argumente Pro- und Contra Staatsüberwachung

Pro:

- Durch den Einsatz von Überwachungstechnologien hat der Staat die Möglichkeit, einen entscheidenden Schritt schneller als die Verbrecher zu sein. Über die Analyse von Verhaltensmustern in Aufenthaltsorten, Anrufen, finanziellen Transaktionen, aufgerufenen Webseiten oder eingekauften Artikeln kann er potenzielle Straftäter ausfindig machen. So können Terroranschläge noch vor dem Versuch im Keim erstickt werden.
- Kriminelle haben die Vorteile der Kommunikation über verschlüsselte Verbindungen längst erkannt. So ist es der Polizei praktisch unmöglich, Gespräche mitzuhören, wenn die Daten mit einer zu starken Verschlüsselung versehen sind. Der Einsatz von Überwachungssoftware wie Trojanern ermöglicht den Behörden, die Kommunikation noch vor der Codierung abzufangen.
- Durch den Einsatz von modernen Überwachungstechnologien können Vorgänge vereinfacht, respektive schneller durchgeführt werden. Beispiele hierfür sind Nacktscanner, Sender zur Maut-Bezahlung/-Überprüfung und RFID-Chips in Identitätskarten.
- Hat die Polizei Zugriff auf die GPS-Daten eines Anrufers, kann im Notfall schneller gehandelt werden, wenn der momentane Aufenthaltsort der jeweiligen Person nicht genau bekannt ist.
- Der Nachweis von Straftaten ist vereinfacht, wenn die Polizei Zugriff auf E-Mail-Kontos respektive den ganzen Nachrichtenverkehr hat. Mit der Vorratsdatenspeicherung bei Internetanbietern hat die Polizei ein effektives Mittel, um Straftätern auch im Nachhinein Delikte nachweisen zu können.

Contra:

- Mehr Überwachung bedeutet auch zugleich mehr Eingriff in die Privatsphäre. Von der Überwachung sind unbescholtene Bürger keines Falls ausgeschlossen. So haben Ermittler theoretisch Einblick in Daten, welche nicht zwingend zur Auflösung eines Strafbestandes benötigt werden. So herrscht immer eine gewisse Unsicherheit, was mit all den angesammelten Daten geschieht und ob diese nicht von Dritten missbraucht werden.
- Fehler oder absichtliche Manipulationen an den Daten sammelnden Systemen können dazu führen, dass Unschuldige verdächtigt oder sogar für nicht begangene Straftaten verurteilt werden. Dass selbst einfache Datenerhebungen fehlerbehaftet sein können, zeigt ein Fall in Deutschland bei dem ein Rentner fälschlicherweise des illegalen Filesharings verdächtigt wurde, weil der ISP Adresse und IP bei der Auskunft für die Staatsanwaltschaft falsch verknüpfte.
- Eine umfassende Überwachung kostet sehr viel Geld. Ob sich diese Investitionen tatsächlich auszahlen, ist fraglich; häufig stehen die

Ausgaben in keinem Verhältnis zu den erzielten Erfolgen. Meist führen die Ausgaben zu Kostendruck an anderer Stelle, beispielsweise wird dann der Personalbestand der Polizei reduziert, was natürlich kontraproduktiv ist.

- Wie am Beispiel des Bundestrojaners in Deutschland aufgezeigt, ist es aussenstehenden Personen möglich, Zugriff auf Systeme zu erhalten, welche mit der Überwachungssoftware versehen wurden. Generell ist so nie ganz auszuschliessen, dass die Überwachungsmöglichkeiten durch Dritte missbraucht werden. Auch aus der Wirtschaft werden regelmässig Interessen an den Datensammlungen gemeldet, z.B. von Verwertungsgesellschaften der Medienverbände.
- Würden alle Staaten eine Infrastruktur aufbauen, um Schlüssel für verschlüsselte Verbindungen und Zugänge zu hinterlegen, bräuchte man enorm viel gut ausgebildetes Personal und sichere Infrastrukturen, um den Betrieb zu gewährleisten. Die Folgen eines Datenlecks in solch einem System durch unsachgemässe Handhabung sind kaum auszumalen.